IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): A gateway device for carrying out a data relaying at a transport or upper layer between a first terminal device and a second terminal device which are capable of carrying out communications through networks with guaranteed data secrecy based on a security association set up therebetween, the gateway device comprising:

a security information management unit configured to obtain and manage information regarding ~~a~~ the security association;

a data receiving unit configured to receive encrypted data from the first terminal device or the second terminal device;

a data decryption unit configured to obtain decrypted data by decrypting the encrypted data by utilizing the information regarding the security association and to check a destination address included in a header of the decrypted data at a time of relaying the communications with guaranteed data secrecy between the first terminal device and the second terminal device;

a data relay unit configured to carry out the data relaying at the transport or upper layer according to the decrypted data;

a data encryption unit configured to encrypt data to be transmitted from the gateway device by utilizing the information regarding the security association, no new destination address being attached to the data to be transmitted; and

a data transmitting unit configured to transmit the encrypted data encrypted by the data encryption unit to the second terminal device or the first terminal device.

Claim 2 (Original): The gateway device of claim 1, wherein the gateway device carries out the data relaying between the first terminal device which is a radio terminal device

accommodated in a radio network and the second terminal device which is a wired terminal device accommodated in a wired network.

Claim 3 (Original): The gateway device of claim 1, wherein the security information management unit manages the information regarding the security association which is provided from the first terminal device or the second terminal device.

Claim 4 (Original): The gateway device of claim 1, wherein the security information management unit manages the information regarding the security association which is provided from a security server for managing security of the data at a time of carrying out the communications of the data of the transport or upper layer between the first terminal device and the second terminal device.

Claim 5 (Original): The gateway device of claim 1, wherein the security information management unit manages the information regarding the security association which is generated by a security server for managing security of the data and distributed from the security server to the first terminal device and the second terminal device.

Claim 6 (Original): The gateway device of claim 1, wherein the security information management unit manages the information regarding the security association which is retrieved from a database by a security server for managing security of the data by using a retrieval key provided with respect to the first terminal device and the second terminal device.

Claim 7 (Original): The gateway device of claim 1, wherein the first terminal device is a mobile terminal device, and the gateway device further comprises:

a handoff control unit configured to transfer the information regarding the security association to a next gateway device when the first terminal moves from an area covered by the gateway device to an area covered by the next gateway device, and to control an operation of the gateway device according to the information regarding the security association which is transferred from a previous gateway device when the first terminal moves from an area of the previous gateway device to an area covered by the gateway device.

Claim 8 (Original): The gateway device of claim 7, wherein the handoff control unit controls the operation of the gateway device also according to a state of the transport or upper layer.

Claim 9 (Original): The gateway device of claim 1, further comprising:

a processing unit configured to obtain decapsulated data by decapsulating encapsulated data received from the first terminal device or the second terminal device, judge whether the data relaying at the transport or upper layer is necessary or not according to the decapsulated data, control the data relay unit to carry out the data relaying at the transport or upper layer when the data relaying at the transport or upper layer is judged as necessary, and encrypt data to be transmitted from the gateway device.

Claim 10 (Previously Presented): A gateway device for carrying out a data relaying at a transport or upper layer between a first terminal device and a second terminal device which are capable of carrying out communications through networks with guaranteed data

authenticity based on a security association set up therebetween, the gateway device comprising:

a security information management unit configured to obtain and manage information regarding ~~a~~ the security association;

a data receiving unit configured to receive data from the first terminal device or the second terminal device;

a data relay unit configured to carry out the data relaying at the transport or upper layer according to the received data;

an authentication information attaching unit configured to attach authentication information to data to be transmitted from the gateway device by utilizing the information regarding the security association; and

a data transmitting unit configured to transmit the data with the authentication information to the second terminal device or the first terminal device.

Claim 11 (Original): The gateway device of claim 10, wherein the gateway device carries out the data relaying between the first terminal device which is a radio terminal device accommodated in a radio network and the second terminal device which is a wired terminal device accommodated in a wired network.

Claim 12 (Original): The gateway device of claim 10, wherein the security information management unit manages the information regarding the security association which is provided from the first terminal device or the second terminal device.

Claim 13 (Original): The gateway device of claim 10, wherein the security information management unit manages the information regarding the security association

which is provided from a security server for managing security of the data at a time of carrying out the communications of the data of the transport or upper layer between the first terminal device and the second terminal device.

Claim 14 (Original): The gateway device of claim 10, wherein the security information management unit manages the information regarding the security association which is generated by a security server for managing security of the data and distributed from the security server to the first terminal device and the second terminal device.

Claim 15 (Original): The gateway device of claim 10, wherein the security information management unit manages the information regarding the security association which is retrieved from a database by a security server for managing security of the data by using a retrieval key provided with respect to the first terminal device and the second terminal device.

Claim 16 (Original): The gateway device of claim 10, wherein the first terminal device is a mobile terminal device, and the gateway device further comprises:

a handoff control unit configured to transfer the information regarding the security association to a next gateway device when the first terminal moves from an area covered by the gateway device to an area covered by the next gateway device, and to control an operation of the gateway device according to the information regarding the security association which is transferred from a previous gateway device when the first terminal moves from an area of the previous gateway device to an area covered by the gateway device.

Claim 17 (Original): The gateway device of claim 16, wherein the handoff control unit controls the operation of the gateway device also according to a state of the transport or upper layer.

Claim 18 (Original): The gateway device of claim 10, further comprising:

a processing unit configured to obtain decapsulated data by decapsulating encapsulated data received from the first terminal device or the second terminal device, judge whether the data relaying at the transport or upper layer is necessary or not according to the decapsulated data, control the data relay unit to carry out the data relaying at the transport or upper layer when the data relaying at the transport or upper layer is judged as necessary, and encrypt data to be transmitted from the gateway device.

Claim 19 (Currently Amended): A method for carrying out a data relaying at a transport or upper layer in a gateway device between a first terminal device and a second terminal device which are capable of carrying out communications through networks with guaranteed data secrecy based on a security association set up therebetween, the method comprising;

obtaining and managing information regarding a security association;

receiving encrypted data from the first terminal device or the second terminal device;

obtaining decrypted data by decrypting the encrypted data by utilizing the information regarding the security association and checking a destination address included in a header of the decrypted data at a time of relaying the communications with guaranteed data secrecy between the first terminal device and the second terminal device;

carrying out the data relaying at the transport or upper layer according to the decrypted data;

encrypting data to be transmitted from the gateway device by utilizing the information regarding the security association, no new destination address being attached to the data to be transmitted; and

transmitting the encrypted data to the second terminal device or the first terminal device.

Claim 20 (Previously Presented): A method for carrying out a data relaying at a transport or upper layer in a gateway device between a first terminal device and a second terminal device which are capable of carrying out communications through networks with guaranteed data authenticity based on a security association set up therebetween, the method comprising:

obtaining and managing information regarding ~~a~~ the security association;

receiving data from the first terminal device or the second terminal device;

carrying out the data relaying at the transport or upper layer according to the received data;

attaching authentication information to data to be transmitted from the gateway device by utilizing the information regarding the security association; and

transmitting the data with the authentication information to the second terminal device or the first terminal device.

Claim 21 (Currently Amended): A computer usable medium having computer readable program codes embodied therein for causing a computer to function as a gateway device for carrying out a data relaying at a transport or upper layer between a first terminal device and a second terminal device which are capable of carrying out

communications through networks with guaranteed data secrecy based on a security association set up therebetween, the computer readable program codes include:

a first computer readable program code for causing said computer to obtain and manage information regarding a security association;

a second computer readable program code for causing said computer to receive encrypted data from the first terminal device or the second terminal device;

a third computer readable program code for causing said computer to obtain decrypted data by decrypting the encrypted data by utilizing the information regarding the security association and to check a destination address included in a header of the decrypted data at a time of relaying the communications with guaranteed data secrecy between the first terminal device and the second terminal device;

a fourth computer readable program code for causing said computer to carry out the data relaying at the transport or upper layer according to the decrypted data;

a fifth computer readable program code for causing said computer to encrypt data to be transmitted from the gateway device by utilizing the information regarding the security association, no new destination address being attached to the data to be transmitted; and

a sixth computer readable program code for causing said computer to transmit the encrypted data to the second terminal device or the first terminal device.

Claim 22 (Previously Presented): A computer usable medium having computer readable program codes embodied therein for causing a computer to function as a gateway device for carrying out a data relaying at a transport or upper layer between a first terminal device and a second terminal device which are capable of carrying out communications through networks with guaranteed data authenticity based on a security association set up therebetween, the computer readable program codes include:

a first computer readable program code for causing said computer to obtain and manage information regarding the security association;

a second computer readable program code for causing said computer to receive data from the first terminal device or the second terminal device;

a third computer readable program code for causing said computer to carry out the data relaying at the transport or upper layer according to the received data;

a fourth computer readable program code for causing said computer to attach authentication information to data to be transmitted from the gateway device by utilizing the information regarding the security association; and

a fifth computer readable program code for causing said computer to transmit the data with the authentication information to the second terminal device or the first terminal device.